UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,251	05/11/2001	Sarver Patel	18	7868

7590 06/14/2006

Docket Administrator (Room 3C-512)
Lucent Technologies Inc.,
600 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/854,251
Filing Date: May 11, 2001
Appellant(s): PATEL, SARVER

Martin I. Finston, Reg. No. 31,613
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/20/06 appealing from the Office action mailed 9/20/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Bellare et al., "Keying Hash Function for Message Authentication", Preliminary Version: Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science, Vol. 1109, Springer-Verlag, (June 1996), pp. 1-19

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4,7-11,14,16, and 19-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al. This rejection is set forth in the prior Office action dated 9/20/2005 and repeated here for convenience.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4,7-11,14,16, and 19-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al. (Keying Hash Function for Message Authentication).

Referring to the rejection of claims 1 and 14, Bellare et al. discloses a method of processing a message for authentication comprising:

determining whether the message fits within an input block of a compression function (See page 7)

performing a single iteration of the compression function using a key and the message as inputs when the message fits within an input block of the compression

function and using a result from the compression function without further iteration thereof to produce a message authentication code (See pages 9-10 and page16)

and using a hash function nested within a keyed hash function to process the message when the message does not fit within an input block of the compression function and using a result from the keyed hash function to produce a message authentication code (See pages 6-7 and page 10)

As per claims 2,7,and 16, Bellare et al. discloses a method comprising the steps of: providing a first portion and a second portion of the message, performing a hash function using the first portion as an input to achieve a result, and performing a keyed hash function using a concatenation of the second portion and the result as inputs (See pages 7-9,13, and 15-16)

As per claims 3 and 10, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is a keyed compression function F (See pages 7-9)

As per claims 4 and 11, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is an iterated hash function F (See pages 7-9)

As per claim 8, Bellare et al. discloses the claimed limitation wherein determining whether the message fits within an input block of a compression function and performing the steps of providing, performing, and performing when the message does not fit within an input block of the compression function (See pages 6-7 and page 10)

As per claim 9 Bellare et al. discloses a method comprising the steps of: determining whether the message fits within an input block of a compression function and performing a single iteration of a compression function using a key and the message as inputs when the message fits within an input block of the compression function (See page 15, Section 6)

Referring to the rejection of claim 19, Bellare et al. discloses a method of processing a message x for authentication comprising:

(a) conditionally processing x to provide an intermediate result y, (See page 10)

(b) compressing x or y with a keyed compression function having a block size (See page 11)

(c) and providing a result of the compressing step for use in a message authentication scheme, wherein (a) comprises using a hash function to compress at least a portion of x and is carried out on condition that x exceeds the block size (See page 11)

As per claim 20, Bellare et al. discloses the claimed limitation wherein (a) comprises providing a first portion and a second portion of the message x, performing a hash function using the first portion as an input to achieve a result, and concatenating the result with the second portion (See pages 7-9)

Referring to the rejection of claim 21, Bellare et al. discloses a message authentication system comprising:

processing circuitry configured to determine whether a message x is larger than an input block size b of a keyed compression function (See pages 9-10)

processing circuitry configured to apply a hash function to compress at least a portion of x, thereby to provide an intermediate result y, the processing circuitry to be activated only in the event that x is larger than b (See page 10)

and processing circuitry configured to compress x or y with the keyed compression function, thereby to provide a result for use in a message authentication scheme (See page 11)

(10) Response to Argument

In general, the appellant's arguments fail to consider the full teachings of the reference in light of the knowledge generally available to one of ordinary skill in the art.

Appellant argues Bellare et al. fails to disclose a hash function nested within a keyed hash function. Bellare et al. discloses a system for securing message authentication, by using key hash functions. The two cryptographic hash functions are HMAC (hashed based message authentication code) and NMAC (nested message authentication code). In order to build a secure message authentication function, a cryptographic hash function must be established, i.e.) hashing data (x) using key (k) is performed by applying the hash function (F) to the concatenation of (k) and (x). The hash function F is keyed with a secret key k_2 and the message x is hashed to the output of $Fk_2(x)$. (See page 8, Section 3) The input message processed by a hash function is nested within a keyed hash function as disclosed in the functionality of an NMAC (nested message authentication code). The output message of $Fk_2(x)$ is padded

according to the block size and the result of $Fk_2(x)$ is keyed with a secret key k_1, and hashed with an outer hash function F. (See page 9, Sections 4-4.1) Therefore, the keyed compression function f which is a secure MAC (message authentication code) on messages of a certain length combined with the keyed iterated hash function F which is collision resistant to attackers, will produce a hash function nested within the keyed hash function known as NMAC (See pages 10-11,Section 4.2)

Appellant argues Bellare et al. fails to disclose performing a single iteration of the compression function using a key and the message as inputs when the message fits within an input block of the compression function without further iteration thereof to produce a message authentication code. Bellare et al. discloses performing a compression function only once because this will prevent extra computation of the key k which is generated or shared the first time and is stored as the actual keys to the function NMAC. This method provides a secure key management for the security of functions within a NMAC. (See pages 14-15, Section 5.3)

Appellant argues Bellare et al. fails to disclose any hash function or MAC-generating function in which two portions of an input message are processed differently, and then concatenated, and the concatenation used as input for further processing. Bellare et al. discloses a keyed hash function of two portions (k) and (x), of an input message. The concatenation of (k) and (x) can be processed by two different methods: hashing data (x) using key (k) or by iterating hash functions using a fixed and known keyed IV. This method will differentiate the two portions (k) and (x) from other data used in input messages. (See page 8, Section 3)

Appellant argues Bellare et al. fails to disclose intermediate results compressed with a keyed compression function based on conditionally processing x or y. Bellare et al. discloses processing a query for the function of $NMAC_k(x)$. After processing (x), the query outputs a pair of variables (x) and (y). After (x) or (y) is keyed with the compression function, the intermediate results will be based upon the variable that was chosen for compressing using the key iterated hash function, and will not always produce the same results because the claim language specifically states "compressing x or y", therefore, the intermediate results are not required, because the results are conditionally processed and will never produce the same result. (See pages 10-11, Section 4.2)

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Courtney Fields

Courtney D. Fields

May 26, 2006

Conferees:

Kim Vu KVu

Emmanuel Moise EMoise